LARA LICENSING AND REGULATORY AFFAIRS CUSTOMER DRIVEN. BUSINESS MINDED.	**Effective Date:**	09-12-2011
	Policy #:	G-21
	Supersedes:	
Subject: **Information Privacy and Security Incident Response**	**Page:**	1 of 4

PURPOSE

This policy specifies actions required of department personnel who report or respond to an information security incident. This policy applies to all individuals or entities using any department IT resources or department data. All department employees are responsible for reporting known or suspected information security events. The Information Privacy Officer (IPO) with DTMB will direct any action deemed necessary to facilitate incident response. The department reserves the right to take any action necessary to protect department resources or preserve evidence.

Those reporting or responding to an incident will follow the Information Privacy and Security Incident Response Policy. All individuals involved in reporting or investigating an information security event shall maintain confidentiality, unless the IPO authorizes information disclosure. The IPO must approve any exceptions to this policy or related procedures.

Reference Documents
LARA Information Privacy and Security Policy
LARA Information Privacy and Security Handling Policy
IT Resources Acceptable Use Policy (Policy 1460.00)

DEFINITIONS

Information Security Event or Information Security Incident - Any event that is known or suspected to have compromised the confidentiality, integrity, or availability of department computer systems, networks, data, or records. Only the IPO may declare an incident.

PROCEDURES

Declaration
All department employees and agents shall report to the IPO any event that may potentially affect the confidentiality, integrity, or availability of department computer systems, networks, data, or records. These information security events may include the loss of control of sensitive department information by unauthorized access, equipment loss, or theft.

Department employees shall promptly report any suspected security events to the IPO in the Director's Office. Bureau directors shall immediately contact the IPO by phone or in person if a high-severity incident may have occurred.

Upon receipt of an event notification, the IPO may declare a formal information security incident. An event will only be considered an incident if the IPO makes this declaration. The IPO shall order whatever actions are necessary to minimize the risk of further loss or disclosure of department information. The IPO shall coordinate response with the Department of Technology, Management and Budget (DTMB) Office of Enterprise Security (OES) for incidents involving IT assets.

Classification

All information security incidents are classified into one of two categories:

- **High severity** incidents include any incident that is known or suspected to meet any of the following criteria:
  - Involves unauthorized access, loss, or theft of a device known to store, process, or transmit sensitive information.
  - Involves an enterprise security device, such as a data center firewall, intrusion detection system, or authentication service.
  - Involves compromise of a networking device, such as a router or switch.
  - Causes security monitoring devices (i.e., intrusion detection system) to report an unauthorized change in the configuration of any device described above.
  - Causes the unavailability of a mission-critical service.
  - Involves a significant number of department systems, indicating a widespread attack.
  - In the judgment of the IPO, poses a high severity risk to department systems or information.
- **Low severity** incidents include any information security incident that does not meet the foregoing high severity criteria, but may have a negative impact on the conduct of department business.

The IPO will determine the initial incident classification, subject to later reclassification.

Response

The highest priority is to protect the department, its clients, and any sensitive information. For all incidents, the priority of response will be to:

- Contain damage from or the spread of the breach
- Determine the extent of the breach
- Preserve evidence
- Eradicate any damage
- Restore systems and services
- Communicate response actions to affected parties

For high severity incidents, DTMB OES staff may take and direct immediate action to protect department systems and data. This includes, but is not limited to, the immediate and complete disconnection of a suspected compromised system from department networks. If this action is necessary, the DTMB OES staff will notify the IPO as soon as practical.

Business Continuity During an Incident Investigation

All work areas should establish a business continuity/disaster recovery plan so they can continue to conduct critical department business during an incident investigation. Business continuity will not take precedence over the activities required to contain damage or preserve evidence. Work areas will handle outages that result from actions to contain incidents according to business continuity/disaster recovery plans. During the response to an incident, meetings and notifications will include the staff responsible for sensitive information involved in the incident. The IPO will direct actions deemed necessary to respond to the incident. This authority includes, as appropriate, communication with other personnel.

Documentation

DTMB OES will periodically prepare a summary report of all information security events, and provide it to the IPO. Upon declaration of an information security incident, DTMB OES will prepare a summary of the relevant technical and operational details and provide it to the IPO. If a high severity incident extends beyond 24 hours, DTMB OES will send the IPO daily updates on the status of the incident and remediation efforts. Within four business days of the conclusion of an incident, DTMB OES will prepare an incident report and provide it to the IPO. The department will comply with all reporting requirements imposed upon it by law or contract. The Director's Office will coordinate any such action.

Evaluation and Testing
The IPO with DTMB staff will coordinate periodic tests of the incident response process and periodic review of the information security incident response policy.

ENFORCEMENT

All department staff must report suspected violations of this policy to the IPO and bureau director. Violations of this policy, including the failure to report one's own improper transmission of sensitive data, are grounds for discipline, up to and including dismissal.